Real-Time Threat Intelligence Dashboard: Aggregating & Visualizing Security Feeds

Introduction

Cybersecurity threats are evolving rapidly, requiring up-to-date monitoring for effective defense. Organizations rely increasingly on dashboards that aggregate real-time threat data to visualize, analyze, and respond to incidents efficiently. This project delivers a web-based threat intelligence dashboard that provides comprehensive situational awareness by combining feeds from multiple public threat intelligence sources with local scanning intelligence.

Abstract

This project implements a real-time dashboard that fetches, aggregates, and visualizes threat data from platforms such as VirusTotal, AlienVault, Shodan, and AbuseIPDB, along with local vulnerability scans. The dashboard offers live statistics, chart-based visualizations, filtering capabilities, and reporting/export features, empowering users to monitor their security posture and react instantly to attacks or anomalies.

Tools Used

- **Backend:** Python (Flask) – for REST API, data aggregation, and local vulnerability scanning.
- **Frontend:** HTML5, CSS3 (Bootstrap), JavaScript (Chart.js, Fetch API).
- **Threat Intelligence APIs:** VirusTotal, AlienVault OTX, Shodan, AbuseIPDB.
- **Miscellaneous:** LocalStorage for client-side data caching; Export/Import as JSON, CSV, PDF; Mocked Gmail integration for alerts (expansion-ready).

Steps Involved in Building the Project

1. **Backend Integration:** Developed Flask backend routes to collect, normalize, and aggregate threat data from external APIs and local vulnerability scanners (SQL injection, XSS, phishing simulation).
2. **Frontend Dashboard Development:** Designed a responsive, user-friendly UI using Bootstrap and Chart.js, featuring dynamic charts, live statistics, search, and filtering.

3. **Real-Time Data Fetch & Storage:** Implemented periodic threat data fetching and storage in localStorage for instant updates and offline access.
4. **User Interaction Features:** Added scanning functionality (files/URLs), export/import options for full threat records, and comprehensive visualization and reporting tools.
5. **Security & Expansion:** Included (mocked) enterprise features – system-wide scans, alerting, email notification modules – making the dashboard scalable for future deployments.

Conclusion

The developed dashboard meets the core requirements of a modern security operations center (SOC) tool: aggregation, visualization, real-time updates, and actionable insights. By combining multiple live threat feeds with local intelligence and user-friendly reporting features, the system enables organizations and individuals to monitor their security stance in real time, streamline incident response, and proactively address vulnerabilities.